CHAPTER

5

USERS, GROUPS, PROFILES, AND POLICIES

After reading this chapter and completing the exercises, you will be able to:

- Understand local users and groups
- Understand user policies
- Understand the local security policies
- Create and manage user accounts
- Create user profiles

Many computers are used by more than one person, especially in business or educational environments. Each person is identified to the computer, and ultimately the network, through a unique user account. Typically, a **user account** contains details about the user, including the user's preferred configuration or environmental settings. To establish a system that maintains details about each user, Windows XP uses named access accounts that are protected with password security. These topics are discussed in detail in this chapter.

Windows XP Professional User Accounts

Windows XP Professional is designed for use as a network client for a Windows NT, Windows 2000, or Windows .NET Server-based domain network, as a member of a workgroup, or as a stand-alone operating system. From a Windows XP Professional system, you are only able to create, configure, and manage **local user accounts**. A local user account exists on a single computer and cannot be used in any manner with domain resources or to gain domain access of any kind. A local user account has no meaning in a domain, it is used for local system access or to gain access to resources on another workgroup member (assuming you have a local account on the other workgroup system). A **domain user account** exists in a domain or to any trusting domain by virtue of being created on a domain controller. A domain user account exists throughout a domain; it can be used on any computer that is a member of that domain. A domain user account is used to gain access to domain resources and can also be used to grant access to local resources.

The information about user accounts and groups discussed in this chapter applies to local user accounts and **local groups** hosted by a Windows XP Professional system. Such local accounts can be maintained whether the host is a standalone system or a network client. When Windows XP Professional is a network client, it can assign access permissions to local resources using domain users and groups, but it is unable to create domain users or groups. Nor is it able to alter the membership of domain groups. For more information on domain-user accounts, see the product-specific documentation and resource kits for Windows NT Server, Windows 2000 Server, or Windows .NET Server.

On a Windows XP Professional system—whether acting as a client in a domain network, a peer-to-peer workgroup, or even as a stand-alone desktop system—user accounts are used to govern or control access. A Windows XP Professional system can exist as a:

- *Stand-alone system*—All users access local resources through a common user account that automatically logs into the system upon boot-up.
- *Stand-alone system*—Each user logs into the system with a unique user account to gain access to local resources.
- *Workgroup member*—Each user logs into the system with a local user account. (When shared resources are accessed on a remote system, a password or credentials for a user account on that remote system must be supplied.)
- *Domain network client*—Each user logs into the system with a unique domain-user account to gain access to domain and local resources.

A user account is employed to uniquely identify a user to the system, using a named user account and a password. Tied to this user account are numerous details about the user, security settings, and preferences. A Windows XP Professional local user account stores details about:

- *Security*—Passwords protect user accounts so only authorized individuals can gain access.

- *Preferences*—A user's environmental settings and configuration preferences can be stored as a **profile**, so no matter where a user connects to the network, the preferred desktop and resources are available.

In addition to these items, a Windows XP Professional system maintains a wide range of security settings and preferences that affect a user account. These include **password policy**, **account lockout policy**, **audit policy**, user rights assignment, **security options**, public key policies, IP security policies, and more. Many of these topics are discussed throughout this chapter.

Operating systems such as Windows XP that can support more than one user are called **multiple-user systems**. Maintaining separate and distinct user accounts for each person is the common feature of all multiple-user systems. Windows XP implements its multiple-user system through the following:

- *Groups*—**Groups** are named collections of users. Each member of a group takes on the access privileges or restrictions defined for that group. Through the use of groups, administrators can manage many users at one time because a group's settings can be defined once and apply to all members of that group. When the group settings are changed or modified, those changes automatically affect every member of that group. Thus, changing each user's account is not necessary. Later in this chapter, you will learn how to create and manage groups.
- *Resources*—On a network or within a standalone system, resources are defined as any useful service or object, including printers, shared directories, and software applications. A resource can be accessible by everyone across the network or be limited to one person on a single machine, and at any level in between. The range of control over resources within Windows XP is astounding. Details on how to manage resources and control who has and who doesn't have access are presented later in this chapter.
- *Policies*—A policy is a set of configuration options that define aspects of Windows XP's security. Security policies are used to define password restrictions, account lockouts, user rights, and event auditing. System policies are defined for a user, computer, or a group to restrict the computing environment. Details on both types of policies are discussed later in this chapter.
- *Profiles*—A profile is a stored snapshot of the environmental settings of a user's desktop, Start menu, and other user-specific details. Profiles can exist on a single computer or be configured to follow a user around a network no matter what workstation is used. **User profiles** are discussed in detail later in this chapter.

Now that you've had a brief overview of the multiple-user system of Windows XP, you'll learn about these topics in more detail.

LOGGING ONTO WINDOWS XP

Windows XP uses **logon authentication** for two purposes: first, to maintain security and privacy within a network; and second, to track computer usage by user account. Each Windows XP user can have a unique user account that identifies that user and contains or references all the system preferences for, access privileges of, and private information about that one user. Thus, Windows XP can provide security and privacy for all users through the mandatory requirement of logon authentication.

Windows XP supports two types of logon: Windows Welcome and classic. The Windows Welcome logon is a completely new logon method to the Windows product line. Windows Welcome is designed for use on standalone or workgroup member systems. When the system boots, a list of user accounts with icons is displayed. To logon, you point and click at a user name. If a password is defined for the account, you'll be prompted to enter it before access is granted. If no password is defined for the account, access is granted immediately. Windows Welcome can be used only on standalone or workgroup Windows XP systems; it is not available for use on domain members.

Another feature of Windows Welcome logon is Fast User Switching, which allows Windows XP Professional to switch users without logging off. User switching is accomplished by clicking Start, Log Off, then clicking Switch User. This returns you to the Windows Welcome logon screen, where you can select another user account. You should notice that the user account you just switched from now has a listing under the account name indicating how many programs are still active. The programs of the account that is not in use are still active and running. Once you finish with the second user account, you can switch to any other account or log off. Logging back onto the system with the user account previously in use restores that desktop environment and all active programs.

The classic logon method is to press Ctrl+Alt+Delete to access the WinLogon security dialog box. However, the Ctrl+Alt+Delete key sequence can be disabled, so the WinLogon security dialog box appears by default upon bootup or user logout. If the system is a domain member, this is the only logon method allowed. By simultaneously pressing the Ctrl, Alt, and Delete keys at the default splash screen, the Logon Information dialog box appears. Here users enter the logon information—user name, password, and domain—then click OK to have the security system validate their information and grant access to the computer. Once users have completed their work, they can log off the computer to make it available for the next user. There is no user-switching available when classic logon is used.

The logon mode is set to classic logon automatically when the Windows XP system becomes a domain member. On a standalone or workgroup member Windows XP system, the logon method is set through the User Accounts applet. Just click the "Change the way users log on or off" command in the quick list, then on the "Select logon and logoff" page, select "Use the Welcome screen" or "Use classic logon." When the

Welcome screen option is selected, you can also optionally select to enable Fast User Switching.

When Windows XP Professional is installed, it automatically creates two default user accounts: Administrator and Guest.

Administrator

The **Administrator account** is the most powerful user account possible within the Windows XP environment. This account has unlimited access and unrestricted privileges to every aspect of Windows XP. The Administrator account has unrestricted ability to manage all security settings, other users, groups, the operating system environment, printers, shares, and storage devices. Due to these far-reaching privileges, the Administrator account must be protected from misuse. Defining a complicated password for this account is highly recommended. You should also rename this account, thereby increasing the difficulty for hackers attempting to discover a valid user name and password.

The Administrator account has the following characteristics:

- It cannot be deleted
- It cannot be **locked out**
- It can be **disabled**
- It can have a blank password (however, this is not recommended)
- It can be renamed
- It cannot be removed from the Administrators local group

Guest

The **Guest account** is one of the least privileged user accounts in Windows XP. This account has limited access to resources and computer activities. Even so, you should set a new password for the Guest account, and it should be used only by authorized one-time users or users with low-security access. Any configuration changes made to the desktop or Start menu are not recorded in the Guest's user profile. If you do allow this account to be used, you should rename it.

The Guest account has the following characteristics:

- It cannot be deleted
- It can be locked out
- It can be disabled (it is disabled by default)
- It can have a blank password (it is blank by default)
- It can be renamed
- It can be removed from the Guests local group

Naming Conventions

Before creating and managing user accounts, you need to understand naming conventions. A **naming convention** is simply a predetermined process for creating names on a network or standalone system. A naming convention should incorporate a scheme for user accounts, computers, directories, network shares, printers, and servers. These names should be descriptive enough so that anyone can figure out to which type of object the name corresponds. For example, you should name computers and resources by department or by use, to simplify user access.

This stipulation of always using a naming convention seems pointless for small networks, but it is rare for small networks to remain small. Most networks grow at an alarming rate. If you begin naming network objects at random, you'll soon forget which resource corresponds to which name. Even with Windows XP's excellent management tools, you'll quickly lose track of important resources if you don't establish a standard way of naming network resources.

The naming convention your organization settles on ultimately doesn't matter, as long as it can always provide you with a useful name for each new network object. To give you an idea of a naming scheme, here are two common rules:

- User names are constructed from the first and last name of the user, plus a code identifying his or her job title or department (i.e., BobScottAccounting).
- Group names are constructed from resource types, department names, location names, project names, and combinations of all four (i.e., Accounting01, AustinUsers, BigProject01, etc.).

No matter what naming convention is deployed, it needs to address the following four elements:

- It must be consistent across all objects.
- It must be easy to use and understand.
- New names should be easily constructed by mimicking the composition of existing names.
- An object's name should clearly identify that object's type.

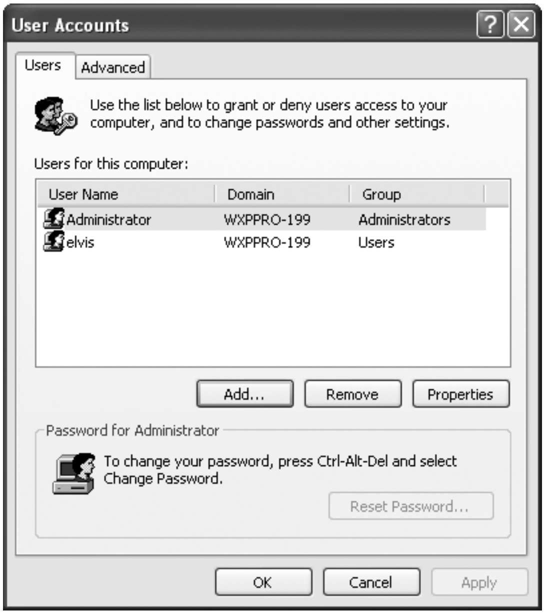
Managing User Accounts

Windows XP Professional actually has two user management interfaces. The first is the User Accounts applet, accessed through the Control Panel, and the second is Local Users and Groups, accessed through the Advanced button on the Advanced tab of the User Accounts applet. The User Accounts applet is used to create a local user account out of an existing domain account. The Local Users and Groups snap-in is used to create local user accounts from scratch.

User Accounts Applet

The User Accounts applet (see Figure 5-1) is used to perform several functions on local user accounts. This applet can be opened only if you are logged into the Windows XP Professional system with the Administrator account, logged with a user account that is a member of the Administrators group, or by providing the username, password, and domain when attempting to launch the applet. (This last method is known as Secondary Logon.) The User Accounts applet has two tabs, Users and Advanced. The Users tab displays all active (i.e., non-disabled) user accounts that can be employed to gain local access. This list details the user name, the domain, and the group memberships of the user account. The term domain in this instance refers to the logical environment where the user account originated. All user accounts created on the Windows XP Professional system have the local computer name listed as its domain (as in WXPPRO-199 in Figure 5-1). All user accounts from a domain (such as created by Windows NT, Windows 2000, or Windows .NET Server) or other networking environment have the name of that domain listed as its domain.

This section on managing user accounts focuses on local user account management while the computer is a domain member. The User Accounts interface functions differently when the system is a stand-alone system or a workgroup member. In those cases, the User Accounts utility becomes a task Wizard where user maintenance is performed through easy to follow task selections.



Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

Users for this computer:

User Name	Domain	Group
Administrator	WXPPRO-199	Administrators
elvis	WXPPRO-199	Users

Password for Administrator

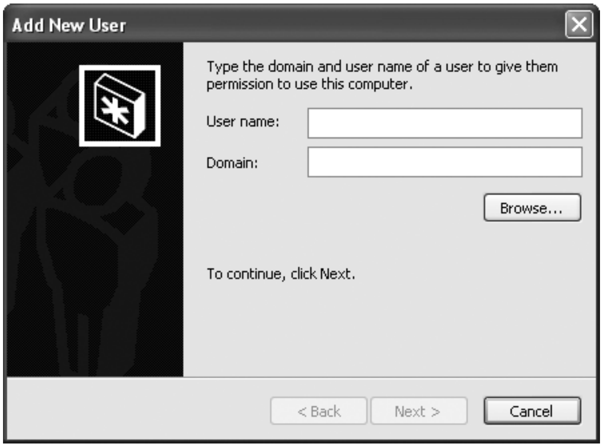
To change your password, press Ctrl-Alt-Del and select Change Password.

Figure 5-1 User Accounts applet, Users tab

To create new local user accounts, you must decide what type of user account to create. On a Windows XP Professional system, there are local user accounts created from scratch locally and there are local user accounts that are just local representations of domain/network user accounts. To create a new local user account from scratch, you'll need to employ Local Users and Groups. To create a local representation of an existing domain/network user account, use the Add button on the User Accounts applet.

Creating a local representation of an existing domain/network user account grants a network user the ability to access resources hosted by the Windows XP Professional system whether or not it is a member of the domain/network. These important user accounts cannot be used to log onto a Windows XP Professional system; they can be used only to access resources over the network hosted on a Windows XP Professional system (i.e., the domain user is authenticated by the domain controller and the local representation of that account is used to gain access to the resources on the client). Plus, the use of local representations allows the administrator or user of a Windows XP Professional system to create a local security configuration of users and groups that does not rely upon the group memberships of the domain/network. However, it is still possible to add domain users and domain groups to local groups.

Clicking the Add button reveals the Add New User Wizard (see Figure 5-2). If you know the name of the user account and the domain of which it is a member, you can type this information in manually. You can also click the Browse button to access the Select User dialog box where you can perform an LDAP query to locate a user. Clicking Next prompts you for the access level to grant the imported user (see Figure 5-3). The selections are:



Add New User

Type the domain and user name of a user to give them permission to use this computer.

User name:

Domain:

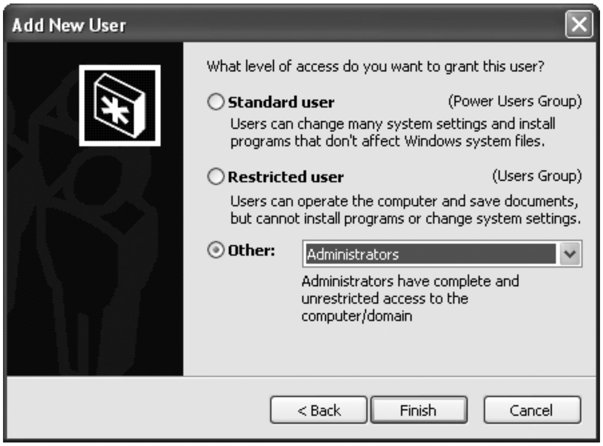
To continue, click Next.

Figure 5-2 Add New User Wizard, user name and domain page

- *Standard user*—Grants the imported user membership into the local Power Users group.

- *Restricted user*—Grants the imported user membership into the local Users group.
- *Other*—Grants the imported user membership into the existing local group selected from the pull-down list.

Once you click Finish on the Wizard, the imported user is added to the list of local users for this computer. To remove an existing user, just select it from the list and click Remove. You'll be prompted to confirm the user account deletion.



What level of access do you want to grant this user?

○ **Standard user** (Power Users Group)
Users can change many system settings and install programs that don't affect Windows system files.

○ **Restricted user** (Users Group)
Users can operate the computer and save documents, but cannot install programs or change system settings.

● **Other:** Administrators
Administrators have complete and unrestricted access to the computer/domain

Figure 5-3 Add New User Wizard, level of access page

The Properties button is used to access basic properties for the selected user account. A locally created user account's Properties dialog box has two tabs, General and Group Membership. The General tab is used to change the user name, full name, and description. The Group Membership tab allows you to change a users group membership. An **imported user account's** Properties only has a Group Membership tab; it does not have a General tab. An imported user account can only be a member of a single group. A locally created group can be a member of more than one group, but the Group Membership tab of the Properties for the user account allow only a single group to be selected. To add a user account to multiple groups requires the use of Local Users and Groups.

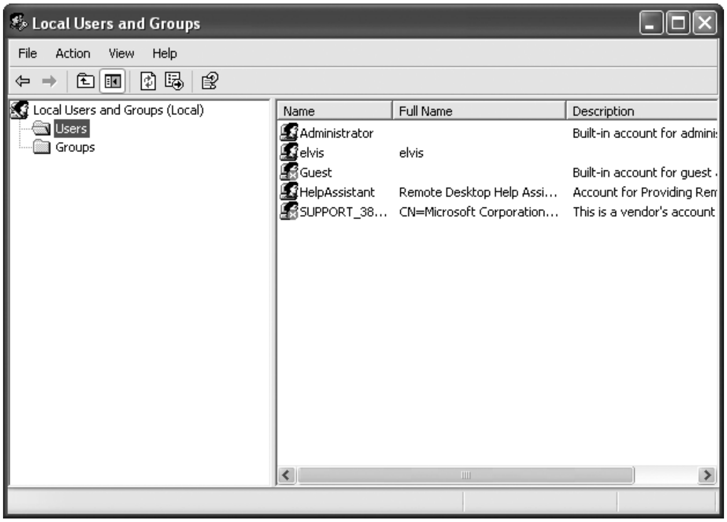
The password for locally created users can be changed using the Reset Password button at the bottom of the User Accounts applet (be sure to select the user account first). You'll be prompted only for the new password and a confirmation of the new password.

Imported user accounts appear in this applet whether or not the Windows XP Professional system is logged into the domain from which the accounts are imported. The only requirement is that the applet be able to communicate with the domain through a network connection. If the Windows XP Professional system is physically disconnected from the network media or the domain is not available, the imported user accounts won't be listed. Once the domain of origin returns, the user accounts reappear.

The Advanced tab of the User Accounts applet grants you access to password and .NET passport management, advanced user management, and secure logon settings. Manage Passwords is used to add, remove, or edit logon credentials for various networks and Web sites. The .NET Passport Wizard is used to define your Microsoft passport account for use in messaging, Microsoft personalized Web pages, and using passport restricted Web sites. Advanced user management is discussed in detail in the next section. The Secure logon setting is just a single checkbox that determines whether the Ctrl+Alt+Delete key sequence is required before the logon dialog box is displayed for the classic logon method.

Local Users and Groups

The Local Users and Groups tool (see Figure 5-4) is accessed by pressing the Advanced button on the Advanced tab of the User Accounts applet or through Computer Management in Administrative Tools. This tool is used to create and manage local users; imported users do not appear in this interface. The console tree hosts only two nodes: Users and Groups. The Users node contains all local user accounts. The Groups node contains all local group accounts.



Name	Full Name	Description
Administrator		Built-in account for admini:
elvis	elvis	
Guest		Built-in account for guest .
HelpAssistant	Remote Desktop Help Assi...	Account for Providing Rem
SUPPORT_38...	CN=Microsoft Corporation...	This is a vendor's account

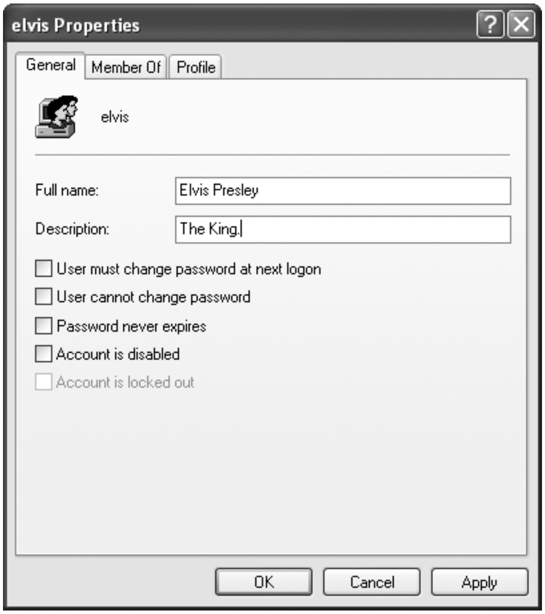
Figure 5-4 Local Users and Groups, Users node

Users

Selecting the Users node displays all existing local user accounts. Initially, the Administrator and Guest account (as seen in Figure 5-4) are displayed. The HelpAssistant and Support accounts are used to enable Remote Assistance and online Help and Support Services, respectively. The details pane lists the name of the user account, the full name of the user, and the description of the account. By selecting a user account and right-clicking, you can access the account's Properties. The Properties dialog box for a local user account has three tabs: General, Member Of, and Profile.

All of the right-click pop-up menu commands described in this chapter also appear in the Action drop-down menu when the appropriate object is selected.

The General tab (see Figure 5-5) of a user account's Properties offers the following:



Full name: Elvis Presley

Description: The King.

□ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

□ Account is locked out

Figure 5-5 A user account's Properties dialog box, General tab

- *Name of user account*—Not customizable through this dialog box.
- *Full Name*—Customizable full name of the person using the account.
- *Description*—Customizable text field to describe the purpose or use of the account.
- *User must change password at next logon*—A checkbox used to force a user to change their password the next time they log onto the system.
- *User cannot change password*—A checkbox that prevents the user from altering his current password.
- *Password never expires*—A checkbox that exempts this user from the account policy that defines the maximum lifetime of a password.
- *Account is disabled*—A checkbox used to turn off an account. This prevents the account from being used but retains it for security auditing purposes.

- *Account is locked out*—A checkbox used by the lockout policy when an account meets the lockout parameters.

The Member Of tab (see Figure 5-6) lists the groups of which this user account is currently a member. To add group memberships, click the Add button. This opens the Select Groups dialog box. From this dialog box, you can type in the name of an existing local group to add this user account to. Or, you can click the Advanced tab, which opens a dialog box that searches for groups and displays a list to select from. To remove a group membership, select it on the Member Of tab and click Remove.

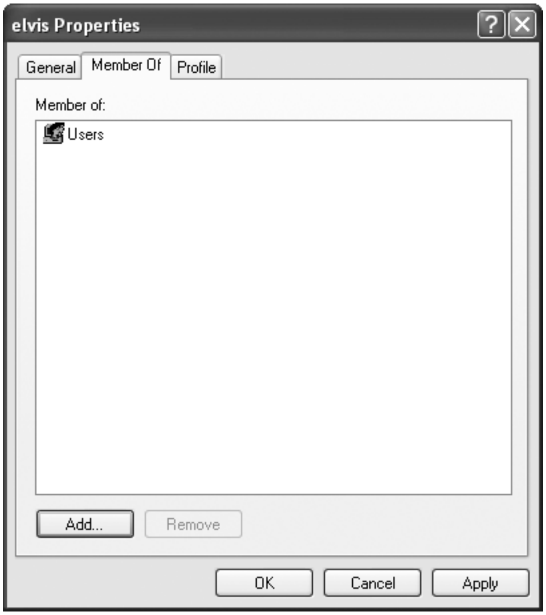
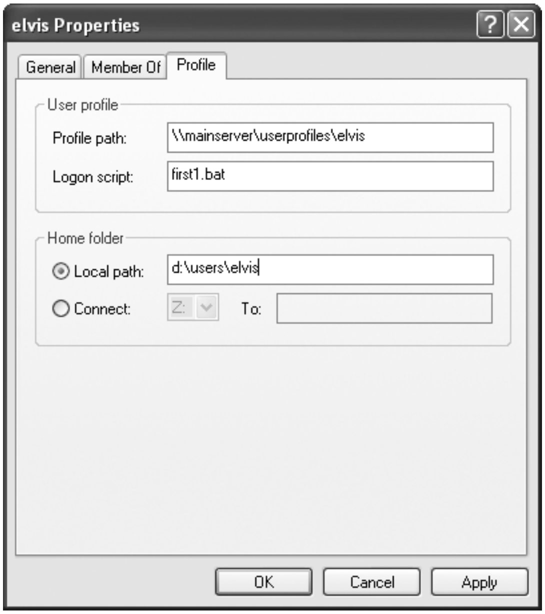


Figure 5-6 A user account's Properties dialog box, Member Of tab

The Profile tab (see Figure 5-7) is used to define the user profile path, logon script, and home folder. Because this is a Windows XP Professional local user, most of the paths used on this tab should be local (i.e., residing on the local computer). Profiles are discussed in detail later in this chapter. The Profile path defines the alternate location where a user's profile is to be stored. By default, user profiles are stored in \Documents and Settings\<*username*>, where <*username*> is the name of the user to whom the profile belongs or applies. The logon script is the local path to a logon script that can map drive letters, launch applications, or perform other command-line operations each time the system boots. The home folder is the default location for the storage of user-created documents and files. By default the home folder is the \Documents and Settings\<*username*>\My Documents folder, but this setting can be used to define an alternate location with either a path statement or with a mapped drive letter to a network share (such as K and \\mainserver\users\steve).



Profile path: \\mainserver\userprofiles\elvis

Logon script: first1.bat

● Local path: d:\users\elvis

○ Connect: Z: To:

Figure 5-7 A user account's Properties dialog box, Profile tab

From within the Local Users and Groups tool, the Properties command from the pop-up menu of a user account is only one of several commands available. The others are:

- *Set Password*—Provides a new password and confirmation; the original password is not required.
- *Delete*—Completely removes a user account from the system, which, once deleted, is not recoverable. Recreating a new account, even with the same name and configuration, is seen as a different account by the system because its SID (security identifier) has changed.
- *Rename*—Changes the name of the user account.
- *Help*—Accesses context-sensitive help.

All other controls on a Windows XP Professional system are defined through the **Local Security Policy** tool (discussed later in this chapter). Microsoft Windows NT, 2000, and .NET Server user management tools offer several other configuration options due to the resources and services available on a domain level. Consult Windows NT, Windows 2000, or Windows .NET Server documentation for details on managing domain users.

Groups

Selecting the Groups node in the Local Users and Groups interface displays all existing local groups, which are named collections of users. All members of a group share the privileges or restrictions of that group. Groups are used to give a specific level of access to multiple users through a single management action. Once a group has access to a resource, users can be added to or removed from that group as needed. The group concept is key to managing large numbers of users and their access to any number of resources. In fact, if you use the group concept effectively, there should be little need to assign access rights to an individual user.

A local user can be a member of multiple groups. Different groups can be assigned different levels of access to the same resources. In such cases, the most permissive of all granted access levels is used, except when access is specifically denied by one or more groups.

As you plan your network security (covered in detail in Chapter 6, "Windows XP Security and Access Controls"), user base, and resource allocation, remember to keep in mind how you will be managing each of these groups. Think about how groups can be paired with resources to provide a wide range of administrative control. Once your resources are in place and all the required groups have been created, most of your administrative tasks involve adding users to or removing them from these groups.

To provide the highest degree of control over resources, Windows XP uses two types of groups: local and global. Local groups exist only on the computer where they are created. **Global groups** exist throughout a domain. Windows XP Professional can create and manage local groups, but not global groups. Windows XP Professional can add only existing global groups to its local groups to grant access to resources. This distinction is very important, as you'll soon see. Local groups can have members who are users or global groups.

To create and manage groups that can be used both within the domain and in trusting domains, you must have a Windows NT, 2000, or .NET Server in a client/server environment. If a Windows XP Professional system is part of a domain, its user tools can add global groups to local groups as members.

On a domain scale, a complete system of links from resources to users can be established. Each resource has one or more local groups assigned to it. Each user is assigned to one or more global groups. Global user groups are assigned to local resource groups. Each local group can be assigned different levels or types of access to the resource. By placing a global group in a local group, you assign all members of that global group the privileges of the local group, i.e., access to a resource. In other words, domain users are members of global groups that are members of local groups that are assigned access permissions to resources. On a standalone or workgroup system, local users are members of local groups that are assigned access permissions to resources.

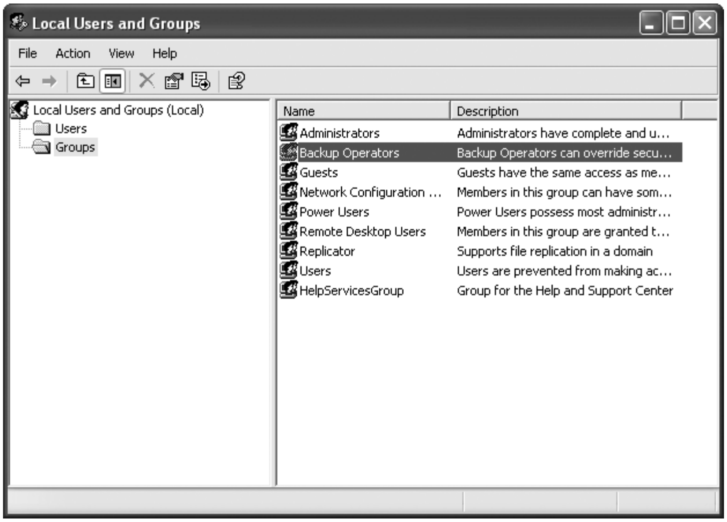
You should plan your group management scheme long before you begin implementation. Planning such a scheme involves applying a naming scheme, dividing users into meaningful groups, and understanding the various levels of access your resources offer. For the group method to be effective, you need to manage all access to resources through groups. Never succumb to the temptation to assign access privileges directly to a user account.

Defining group members is often the most time-consuming process of group management. A group should be formed around a common job position, need of resource, or even geographic location. Some existing groupings you can transform into Windows XP groups are:

- Organizational functioning units, workgroups, or departments
- Authorized users of network programs and applications
- Events, projects, or special assignments
- Authorized users of network resources
- Location or geography
- Individual function or job description

As stated, local groups exist only on the computer where they are created. On each computer, all local groups must have a unique name. You can duplicate the names of local groups on different computers, but they are still separate, distinct groups. We don't recommend using the same name twice on any network, even if the architecture allows it.

Windows XP Professional has several default groups. When the groups node is selected in the Local Users and Groups interface, these default groups (as seen in Figure 5-8) are displayed. The default groups are:



Name	Description
Administrators	Administrators have complete and u...
Backup Operators	Backup Operators can override secu...
Guests	Guests have the same access as me...
Network Configuration ...	Members in this group can have som...
Power Users	Power Users possess most administr...
Remote Desktop Users	Members in this group are granted t...
Replicator	Supports file replication in a domain
Users	Users are prevented from making ac...
HelpServicesGroup	Group for the Help and Support Center

Figure 5-8 Local Users and Groups, Groups node

- *Administrators*—Members of this group have full access to the computer. The Local Administrator is always a member; additionally, if the system is a member of a domain, the Domain Admins group is a member.

- *Backup Operators*—Members of this group can back up and restore all files and folders on a system. It has no default members.
- *Guests*—Members can operate the computer and save files, but cannot install programs or alter system settings. Default member is the Guest account.
- *Network Configuration Operators*—Members can configure network components. It has no default members.
- *Power Users*—Members can modify the computer, create user accounts, share resources, and install programs, but cannot access files that belong to other users. It has no default members.
- *Remote Desktop Users*—Members can logon remotely.
- *Replicator*—This group is used by special user accounts to facilitate directory replication between systems and domains. It has no default members.
- *Users*—Members can operate the computer and save files, but cannot install programs, modify user accounts, share resources, or alter system settings. Default members are the Authenticated Users group (a non-configurable default group) and the Domain Users group if connected to a domain. By default, Windows XP adds all new local user accounts to this group.
- *HelpServicesGroup*—A specialty group used by the Help and Support Center.

The Properties dialog box for a user group allows you to change its description and alter its membership. You can add members to a group from the list of local user accounts or from the list of domain users accounts. Imported user accounts are not listed in this interface. Groups can also be deleted or renamed by selecting the command from the right-click pop-up menu.

New groups are created using the New Group command that appears in the right-click pop-up menu when the cursor is over a blank area of the details pane. When creating a new group, you must provide the group name, a description of the group, and add members.

System Groups and Other Important Groups

Windows XP Professional has several built-in system-controlled groups. System-controlled groups are pre-existing groups that you cannot manage but that appear in dialog boxes when assigned group membership or access permissions. These groups are used by the system to control or place restrictions on specific groups of users based on their activities. These groups include: Anonymous Logon, Batch, Creator Group, Creator Owner, Dialup, Everyone, Interactive, Local Service, Network, Network Service, Remote Interactive Logon, Service, System, and Terminal Server User.

User Profiles

A user profile is a collection of desktop and environmental configurations on a Windows XP system for a specific user or group of users. By default, each Windows XP computer maintains a profile for each user who has logged on to the computer, except for Guest accounts. Each user profile contains information about a particular user's Windows XP configuration. Much of this information is about settings the user can configure, such as color scheme, screen savers, and mouse and keyboard layout.

The material stored in a user profile includes:

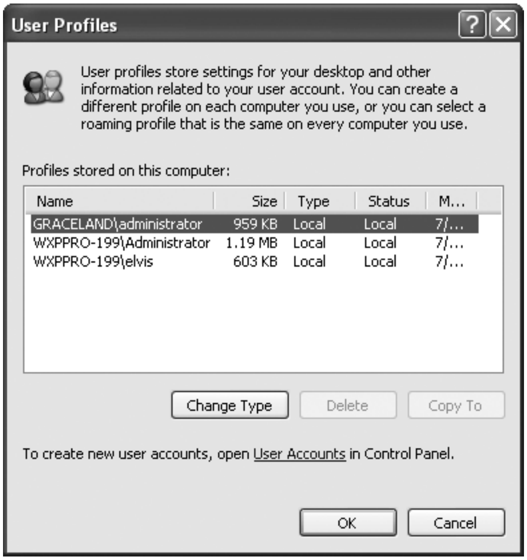
- *Application Data*—A directory containing user-specific data, such as for Internet Explorer or Outlook
- *Cookies*—A directory containing cookies accepted by the user through their browser
- *Desktop*—A directory containing the icons displayed on the user's desktop
- *Favorites*—A directory containing the user's list of URLs from Internet Explorer
- *Local Settings*—A directory containing user-specific history information and temporary files
- *My Documents*—A directory containing user-created data
- *NetHood*—A directory containing user-specific network mappings
- *PrintHood*—A directory containing user-specific printer mappings
- *My Recent Documents*—A directory containing user-specific links to last accessed resources
- *SendTo*—A directory containing user-specific links used in the Sent To command of the right-click pop-up menu
- *Start Menu*—A directory containing the user-specific Start menu layout
- *Templates*—A directory containing user-specific templates
- *NTUSER.DAT*—A file containing Registry information specific to the user
- *NTUSER.DAT.LOG*—A transaction log file that ensures the profile can be re-created in the event of a failure
- *NTUSER.INI*—A file containing profile-related settings, such as what directories should not be uploaded to a roaming profile

Optionally, an administrator can force users to load a so-called **mandatory profile**. Users can adjust this profile while they're logged on, but all changes are lost as soon as they log off—that is, the settings assigned by the mandatory profile are restored the next time that user logs on. A mandatory profile is created by manually renaming the

NTUSER.DAT file to NTUSER.MAN. This technique provides a way for administrators to control the look and feel of shared accounts, or to restrict non-power users from exercising too much influence over their desktops.

User profiles are managed through the System applet. On the Advanced tab, clicking the Settings button under the User Profiles heading opens the User Profiles dialog box (see Figure 5-9). This dialog box lists all profiles for users who have logged into the Windows XP Professional system. This dialog box displays the name of the user account, along with defining its domain of origin, the disk space consumed by the profile, the profile type, status, and when it was last changed. Profiles can be of two types: local or roaming.

Anytime a user logs onto the system and that user account does not already have a user profile, one is created for them. This is done by duplicating the contents of the Default User profile. The All Users profile contains common elements that will appear in every user's environment, such as common Start menu items.



User Profiles

User profiles store settings for your desktop and other information related to your user account. You can create a different profile on each computer you use, or you can select a roaming profile that is the same on every computer you use.

Profiles stored on this computer:

Name	Size	Type	Status	M...
GRACELAND\administrator	959 KB	Local	Local	7/...
WXPPRO-199\Administrator	1.19 MB	Local	Local	7/...
WXPPRO-199\elvis	603 KB	Local	Local	7/...

To create new user accounts, open User Accounts in Control Panel.

Figure 5-9 User Profiles dialog box

Local Profiles

A local profile is a set of specifications and preferences for an individual user, stored on a local machine. Windows XP provides each user with a folder containing their profile settings. Individual profiles are stored in the \Documents and Settings directory. A different location for the Profiles directory can be specified through the Local Users and Groups tool.

Local profiles are established by default for each user who logs onto a particular machine, and reside in the *%username%* subdirectory beneath the \Documents and Settings directory.

There is no single tool that permits all user profile information to be manipulated abstractly. There are only two ways to create a user profile. The first method is to logon as a user and arrange information as needed. Upon logout, this information becomes that user's local profile, which can then be transformed into a roaming profile. The second method is to assign a mandatory profile to that user from an existing definition. Even this must be set up by example, rather than through explicit controls.

Windows XP Professional local users (including imported users) have only local profiles. It is not possible to transform a local user's local profile to a roaming profile. However, a domain user account that logs onto a Windows XP Professional system will have a local profile created the first time they log on (assuming that user does not already have a roaming profile on the network). This local profile for the domain user can be transformed into a roaming profile.

Roaming Profiles

A roaming profile resides on a network server to make it broadly accessible. When a user whose profile is designated as roaming logs onto any Windows XP system on the network, that profile is automatically downloaded when the user logs on. This process avoids having to store a local profile on each workstation that a user uses. The disadvantage to using this kind of profile is that if a user's roaming profile is large, logging on to the network can take a long time because that information must be copied across the network each time that user logs on. In addition, any changes made to the user's profile are uploaded across the network when the user logs off.

The default path designation for a roaming profile is \\*computername**username* (*computername* is typically a network server, but not necessarily a domain controller). To create a roaming profile, it is necessary to use the "Copy to" button that appears in the User Profile tab of the System applet on a machine where a local profile for the user already exists. The destination for that copy operation must match the path that defines where the roaming profile resides (as manually defined in the user account); this is the mechanism that tells the startup module where to find a user's roaming profile. Once a local profile is present on a client, such as a Windows XP Professional system, you must use the System applet on that system to copy the profile to a network file server. Then, you must access the Active Directory Users and Computers tool on a domain controller to alter the profile path for the domain user account. You can create a roaming user profile for a local user by modifying the profile path for that user account through the Local Users and Groups tool.

Local Security Policy

Windows XP has combined several security and access controls into a centralized policy. This centralized policy is called the group policy. There is a local security policy (i.e., a local group policy) for the local system and within a domain. Group policies can be defined for the domain, sites, and organizational units (OUs). All of these group policy types can be managed from a Windows 2000 or .NET Server system, but only the local computer group policy can be managed from a Windows XP Professional system.

Group policies are applied in the following manner:

1. Any existing legacy Windows NT 4.0 NTCONFIG.POL file is applied.
2. Any unique local group policy is applied (read local group-policy instead of local-group policy).
3. Any site group policies are applied.
4. Any domain group policies are applied.
5. Any organizational units (OU) group policies are applied.

Group policies are applied upon bootup and each time a user logs on. Group policies are refreshed every 90 minutes on Windows XP Professional if there are any changes and every 16 hours if there aren't.

The order of application of these policies is important because contradictory settings in the latter policies override the settings of the former policies. The cumulative result of this priority application of group policy is known as the effective policy. On Windows XP Professional systems, the effective policy is either all of these group policies properly combined when logged on with a domain user account or only the local group policy (the local group policy applies whether or not a user is logged on).

The Local Security Policy tool is used to edit the local group policy on a Windows XP Professional system. This tool is accessed from the Administrative Tools applet from the Control Panel. The local group policy consists of several sub-policies, including password, account lockout, audit, user rights, security options, public key, and IP security (see the "Windows XP Security and Access Controls" section in Chapter 6 for details on public key and IP security).

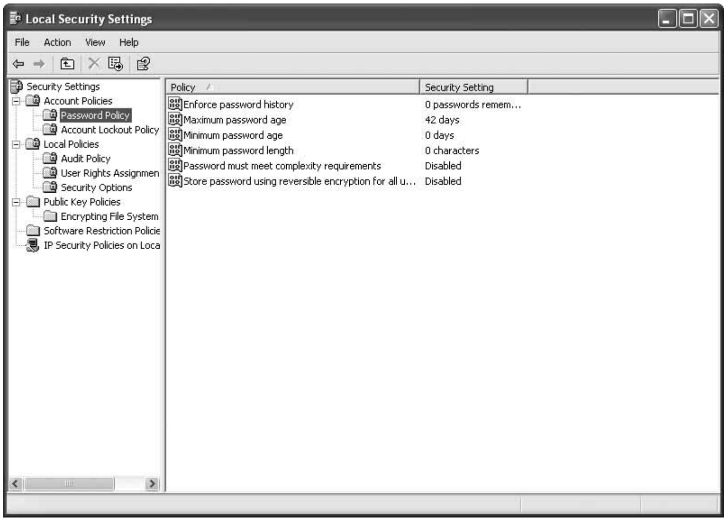
In the details section of the Local Security Policy tool, notice that each specific policy item is listed with both its local setting and its effective setting. Local settings apply when no one is logged on or when logged on with a local user account. Effective settings apply when logged on with a domain user account. For all policy items, only the local default setting is listed because the effective setting varies based on network configuration.

Password Policy

The Password Policy (see Figure 5-10) defines the restrictions on passwords. This policy is used to enforce strong passwords for a more secure environment. The items in this policy are:

- *Enforce password history: 0 Passwords*—Maintaining a password history prevents reuse of old passwords; a setting of 5 or greater for this item is recommended.
- *Maximum Password Age: 42 Days*—Defines when a password expires and must be replaced; a setting of 30, 45, or 60 days is recommended.

- *Minimum Password Age: 0 Days*—Defines the least amount of time that can pass between password changes; a setting of 1, 3, or 5 days is recommended.
- *Minimum Password Length: 0 Characters*—Sets the number of characters that must be present in a password; a setting of 6 or more is recommended.



Policy	Security Setting
Enforce password history	0 passwords remem...
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store password using reversible encryption for all u...	Disabled

Figure 5-10 Local Security Settings, Password Policy selected

- *Passwords must meet complexity requirements of installed password filter: Disabled*—Determines whether passwords must comply with installed password filters. See the *Microsoft Windows .Net Server Resource Kit* for details.
- *Store passwords using reversible encryption for all users in the domain: Disabled*—Determines whether CHAP (Challenge Handshake Authentication Protocol) is used to encrypt passwords; leave this disabled unless required by a client.

Account Lockout Policy

The Account Lockout Policy defines the conditions that result when a user account is locked out. Lockout is used to prevent brute force attacks against user accounts. The items in this policy are:

- *Account lockout threshold: 0 Invalid logon attempts*—Defines the number of failed logons that must occur before an account is locked out; a setting of 3 to 5 is recommended.
- *Account lockout duration: Not Applicable (defaults to 30 minutes once Account Lockout Threshold is defined)*—Defines the length of time an account remains locked out; a value of 0 causes locked-out accounts to require administrative action to unlock, a setting of 30 minutes to 2 hours is recommended.

- *Reset account lockout counter after: Not Applicable (defaults to 30 minutes once Account Lockout Threshold is defined)*—Defines the length of time that must expire before the failed logon attempts for a user account is reset; a setting of 15 minutes is recommended.

Audit Policy

The Audit Policy defines the events that are recorded in the Security log of the Event Viewer. Auditing is used to track resource usage. Each item in this list can be set to audit the Success and/or Failure of the event. The items in this policy are as follows:

- *Audit account logon events: No auditing*—Audits authentication of a user account on this system when it is used to logon or off another system.
- *Audit account management: No auditing*—This item audits the changes to user accounts and group memberships.
- *Audit directory service access: No auditing*—Audits access to Active Directory objects.
- *Audit logon events: No auditing*—Audits user account logins, logoffs, and establishment of network connections.
- *Audit object access: No auditing*—Audits resource access.
- *Audit policy change: No auditing*—Audits changes to the security policy.
- *Audit privilege use: No auditing*—Audits use of special rights or privileges.
- *Audit process tracking: No auditing*—Audits the activity of processes.
- *Audit system events: No auditing*—Audits system-level activities.

For more details about auditing, see Chapter 6.

User Rights Policy

The **User Rights Policy** defines which groups or users can perform the specific privileged action. The items in this policy are:

- *Access this computer from the network*—Everyone, Users, Power Users, Backup Operators, Administrators
- *Act as part of the operating system*—None
- *Add workstation to domain*—None
- *Adjust memory quotas for a process*—Local Service, Network Service, Administrators
- *Allow logon through Terminal Services*—Administrators, Remote Desktop Users

- *Back up files and directories*—Backup Operators, Administrators
- *Bypass traverse checking*—Everyone, Users, Power Users, Backup Operators, Administrators
- *Change the system time*—Power Users, Administrators
- *Create a pagefile*—Administrators
- *Create a token object*—None
- *Create permanent shared objects*—None
- *Debug programs*—Administrators
- *Deny access to this computer from the network*—Guest, SUPPORT
- *Deny logon as a batch job*—SUPPORT
- *Deny logon as a service*—None
- *Deny logon locally*—Guest, SUPPORT
- *Deny logon through Terminal Services*—None
- *Enable computer and user accounts to be trusted for delegation*—None
- *Force shutdown from a remote system*—Administrators
- *Generate security audits*—Local Services, Network Service
- *Increase quotas*—Administrators
- *Load and unload device drivers*—Administrators
- *Lock pages in memory*—None
- *Logon as a batch job*—None
- *Logon as a service*—Network Service
- *Logon locally*—Guest account, Users, Power Users, Backup Operators, Administrators
- *Manage auditing and security log*—Administrators
- *Modify firmware environment values*—Administrators
- *Perform volume maintenance tasks*—Administrators
- *Profile single process*—Power Users, Administrators
- *Profile system performance*—Administrators
- *Remove computer from docking station*—Users, Power Users, Administrators
- *Replace a process level token*—LOCAL SERVICE, NETWORK SERVICE
- *Restore files and directories*—Backup Operators, Administrators

- *Shut down the system*—Users, Power Users, Backup Operators, Administrators
- *Synchronize directory service data*—None
- *Take ownership of files or other objects*—Administrators

User Rights are enabled as defined in the previous list by default. You can alter this configuration through the User Rights Assignment section of the Local Security Policy. Troubleshooting user rights is a process of test, re-configure, and retest. If you suspect an action cannot be performed that should be possible, test, re-set the associated user right, re-log on that user, and try the action again. Be sure to double-check any file or object permissions associated with the action because it can be blocked by lack of access rather than a user right.

For more details on these user rights, consult the *Microsoft Windows XP Professional Resource Kit*.

Security Options

Security Options defines and controls various security features, functions, and controls of the Windows XP environment. The items in this policy are:

- Accounts: Administrator account status: Enabled
- Accounts: Guest account status: Disabled
- Accounts: Limit local account use of blank passwords to console logon only: Enable
- Accounts: Rename administrator account: Administrator
- Accounts: Rename guest account: Guest
- Audit: Audit the access of global system objects: Disabled
- Audit: Audit use of Backup and Restore privilege: Disabled
- Audit: Shut down system immediately if unable to log security audits: Disabled
- Devices: Allow undock without having to logon: Enabled
- Devices: Allowed to format and eject removable media: Administrators
- Devices: Prevent users from installing printer drivers: Disabled
- Devices: Restrict CD-ROM access to locally logged-on user only: Disabled
- Devices: Restrict floppy access to locally logged-on user only: Disabled
- Devices: Unsigned driver installation behavior: Warn but allow installation
- Domain controller: Allow server operators to schedule tasks: Not defined
- Domain controller: LDAP server signing requirements: Not defined

- Domain controller: Refuse machine account password changes: Not defined
- Domain member: Digitally encrypt or sign secure channel data (always): Enabled
- Domain member: Digitally encrypt secure channel data (when possible): Enabled
- Domain member: Digitally sign secure channel data (when possible): Enabled
- Domain member: Disable machine account password changes: Disabled
- Domain member: Maximum machine account password age: 30 days
- Domain member: Require strong (Windows 2000 or later) session key: Disabled
- Interactive logon: Do not display last user name: Disabled
- Interactive logon: Do not require CTRL+ALT+DEL: Not defined
- Interactive logon: Message text for users attempting to logon: blank
- Interactive logon: Message title for users attempting to logon: Not defined
- Interactive logon: Number of previous logons to cache (in case domain controller is not available): 10 logons
- Interactive logon: Prompt user to change password before expiration: 14 days
- Interactive logon: Require Domain Controller authentication to unlock workstation: Disabled
- Interactive logon: Smart card removal behavior: No Action
- Microsoft network client: Digitally sign communications (always): Disabled
- Microsoft network client: Digitally sign communications (if server agrees): Enabled
- Microsoft network client: Send unencrypted password to third-party SMB server: Disabled
- Microsoft network server: Amount of idle time required before suspending session: 15 minutes
- Microsoft network server: Digitally sign communications (always): Disabled
- Microsoft network server: Digitally sign communications (if client agrees): Disabled
- Microsoft network server: Disconnect clients when logon hours expire: Enabled
- Network access: Allow anonymous SID/Name translation: Disabled

- Network access: Do not allow anonymous enumeration of SAM accounts: Enabled
- Network access: Do not allow anonymous enumeration of SAM accounts and shares: Disabled
- Network access: Do not allow storage of credentials or .NET Passports for network authentication: Disabled
- Network access: Let Everyone permissions apply to anonymous users: Disabled
- Network access: Named Pipes that can be accessed anonymously: COMNAP, COMNODE, SQL/QUERY, SPOOLSS, LLSRPC, EPMAPPER, LOCATOR, TrkWks, TrkSvr
- Network access: Remotely accessible Registry paths: System\CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\Print\Printers, System\CurrentControlSet\Control\Server Applications, System\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP Server, Software\Microsoft\Windows NT\Current Version, System\CurrentControlSet\Control\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUserConfig
- Network access: Shares that can be accessed anonymously: COMCFG, DFS$
- Network access: Sharing and security model for local accounts: Guest only—local users authenticate as Guest
- Network security: Do not share LAN Manager has value on next password change: Disabled
- Network security: Force logoff when logon hours expire: Disabled
- Network security: LAN Manager authentication level: Send LM & NTLM responses
- Network security: LDAP client signing requirements: Negotiate signing
- Network security: Minimum session security for NTLM SSP based (including secure RPC) clients: No minimum
- Network security: Minimum session security for NTLM SSP based (including secure RPC) servers: No minimum
- Recovery console: Allow automatic administrative logon: Disabled
- Recovery console: Allow floppy copy an access to all drives and all folders: Disabled

- Shutdown: Allow system to be shut down without having to logon: Enabled
- Shutdown: Clear virtual memory pagefile: Disabled
- System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing: Disabled
- System objects: Default owner for objects created by members of Administrators group: Object creator
- System objects: Require case insensitivity for non-Windows subsystems: Enabled
- System objects: Strengthen default permissions of internal system objects (e.g., Symbolic Links): Enabled

For more details on these security options, consult the *Microsoft Windows XP Professional Resource Kit*.

TROUBLESHOOTING CACHED CREDENTIALS

Windows XP Professional automatically caches a user's credentials in the Registry when a domain logon or .NET passport logon is performed. Caching of credentials is used to enable a single sign-on requirement. This process allows a user access to shared resources from the network without having to re-authenticate each time. By default, Windows XP caches credentials for the last 10 users who logged on. Caching of credentials can be disabled through two means from the Windows XP Professional client. One method is to enable the following group policy setting: Network access: Do not allow Stored User Names and Passwords to save passwords or credentials for domain authentication (this setting is located within Computer Configuration, Windows Settings, Security Settings, Local Policies, Security Options). The second method is to set the "cachedlogonscount" Registry value within the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon key to 0. It is set to 10 by default. Troubleshooting credential caching typically involves disabling the feature and rebooting the system to clear out the previously cached information. Not caching credentials is a more secure configuration.

In addition to caching logon credentials, Windows XP also retains usernames and passwords for resources. These cached resource access credentials are managed through a utility called "Stored User Names and Passwords." This utility is accessed through the User Accounts applet. If you are a domain member, select the Advanced tab and click Manage Passwords. If you are not a domain member, click the account name and click Manage my network passwords from the Related Tasks lists. From this simple window, you can add, remove, or edit stored credentials. If either of the changes to disable caching of credentials is implemented, Windows XP will also disable Stored User Names and Passwords from retaining resource access logon credentials.

If you discover that you are being authenticated as the wrong user account or with the wrong access level, you should remove the stored account information for that server or domain. The next time you attempt to access the resource, you should be prompted for your credentials. Another problem is being unable to access resources to which you previously had access. In many cases, this may indicate that your account has expired or your password must be changed. To remedy this type of situation, edit your account credentials to reflect the updated account information. Yet another problem might occur when you obtain access to a resource to which you should not have access. In most cases, this indicates that stored credentials should be deleted to remove this unauthorized access. You should even consider disabling the storage of credentials by enabling the security option within group policy.

File and Settings Transfer Wizard

The Files and Settings Transfer Wizard is used to move your data files and personal desktop settings from another computer to your new Windows XP Professional system. You must have some sort of network connection between the two systems; this can be a standard LAN connection, a direct cable connection, or a dial-up connection. Using this Wizard, you can transfer files from Windows 95, 98, SE, Me, NT, 2000, or XP systems. To launch this Wizard, select Start|All Programs|Accessories|System Tools.

To use the Wizard, you must be able to execute it on both the new and old systems. If you have the Windows XP Professional CD on hand, you can launch the Wizard from the \Support\Tools folder (it's called FASTWiz.exe). If you don't have the CD, you can create a Wizard disk from which you can launch the Wizard on the old system. The process involved in using the Files and Settings Transfer Wizard is put to use in Hands-on Project 5-10.

The transfer process can take considerable time. The default settings are to grab nearly every file that is not native to the Windows OS or installed applications. This means every document, sound, movie, image, or other file type will be included in the default file selection. There is an option to custom-select the files to transfer. If you have a significant amount of files, you may want to use this option to reduce the time and space consumed by the transfer process.

Chapter Summary

❒ In this chapter, you learned about local users and groups. Windows XP Professional can employ three types of users: locally created users, imported users, and domain users. A user account stores preference settings for each individual who uses a computer. Each user can have his own profile that retains all of his preferred desktop settings. Users are collected into groups to simplify management and grant access or privileges. Users and groups are managed through the User Accounts applet and the Local Users and Groups utility. Windows XP Professional has two built-in users:

Administrator and Guest, and several built-in groups. Some groups allow you to customize their membership; others are system-controlled groups with memberships that cannot be customized.

- User profiles can be local or roaming. User profiles store a wide variety of personalized or custom data about a user's environment. A user profile can be mandatory just by changing NTUSER.DAT to NTUSER.MAN.
- The Local Security Policy is used to manage password, account lockout, audit, user rights, security options, and more. These controls aid in enforcing security and controlling who is able to perform specific actions on the system.

KEY TERMS

account lockout policy — Defines the conditions that result in a user account being locked out.

Administrator account — The most powerful account possible within the Windows XP environment.

audit policy — Defines the events that are recorded in the Security log of the Event Viewer.

disabled — The state of a user account, which is retained on the system but cannot be used to logon.

domain user account — A user account that can be used throughout a domain.

global group — A group that exists throughout a domain. A global group can be created only on a Windows Server system.

groups — A named collections of users.

Guest account — One of the least privileged user accounts in Windows XP.

imported user account — A local account created by duplicating the name and password of an existing domain account. An imported account can be used only when the Windows XP Professional system is able to communicate with the domain of the original account.

local groups — A group that exists only on the computer where it was created. A local group can have users and global groups as members.

Local Security Policy — The centralized control mechanism that governs password, account lockout, audit, user rights, security options, public key, and IP security.

local user account — A user account that exists on a single computer.

locked out — The state of a user account that is disabled due to logon attempts that have repeatedly failed.

logon authentication — The requirement to provide a name and password to gain access to the computer.

mandatory profile — A user profile that does not retain changes once the user logs out. Mandatory profiles are used to maintain a common desktop environment for users.

multiple-user system — An operating system that maintains separate and distinct user accounts for each person.

naming convention — A standardized regular method of creating names for objects, users, computers, groups, etc.

password policy — Defines the restrictions on passwords.

profile — See *user profile*.

security options — Defines and controls various security features, functions, and controls of the Windows XP environment.

user account — A named security element used by a computer system to identify individuals and to record activity, control access, and retain settings.

user profile — A collection of user-specific settings that retain the state of the desktop, Start menu, color scheme, and other environmental aspects across logons.

User Rights Policy — Defines which groups or users can perform the specific privileged action.

Review Questions

1. Windows XP Professional is able to create and manage what types of user accounts?
   a. Local
   b. Domain
   c. Imported
   d. Global
2. What types of user accounts can be used on a Windows XP Professional system?
   a. Local
   b. Domain
   c. Imported
   d. Global
3. When not connected to a network, what types of user accounts can be employed on a Windows XP Professional system?
   a. Local
   b. Domain
   c. Imported
   d. Global
4. A Windows XP Professional is an operating system that can allow more than one user account to log onto a single system simultaneously. True or False?

5. Which of the following are true of groups?
   a. Several default groups are built into Windows XP
   b. Are named collections of users
   c. The system groups can be deleted through the Local Users and Groups tool
   d. Used to simply the assignment of permissions
6. Why does Windows XP require logon authentication?
   a. To prevent the spread of viruses
   b. To track computer usage by user account
   c. To maintain security
   d. To promote a naming scheme
7. Which of the following are true for both the Administrator account and the Guest account?
   a. Cannot be deleted
   b. Can be locked out
   c. Cannot be disabled
   d. Can be renamed
8. When logged on under the Guest account, a user has the same access as other members of what group?
   a. Authenticated Users
   b. Users
   c. Power Users
   d. Everyone
9. Imported user accounts can be managed through what interface?
   a. User Manager for Domains
   b. User Accounts
   c. Local Users and Groups
   d. Active Directory Users and Computers
10. Which of the following are true of imported users?
    a. Can only be a member of a single group
    b. You can change their password
    c. Exist only when their domain of origin is present online
    d. Are used to grant domain users access to the local resources

11. When creating a new user through the User Accounts applet, the Restricted user selection makes the new user a member of what group?
    a. Guests
    b. Power Users
    c. Users
    d. Backup Operators
12. To configure more than one group membership for a local user account requires the use of the User Accounts applet. True or False?
13. When the control item under Secure logon on the Advanced tab of the Users and Password applet is selected, not only is Ctrl+Alt+Delete not required, but the last user account to successfully logon is automatically re-used to log onto the system. True or False?
14. You create several new user accounts. You tell everyone they need to logon and change their password to something other than the dummy password you entered to create the account. In the past you've discovered that most users forget to change the password. How can you force them to make this change?
    a. User cannot change password
    b. User must change password at next logon
    c. Password never expires
    d. Account is disabled
15. On a Windows XP Professional client, what types of profiles can be used?
    a. Local
    b. Roaming
    c. Mandatory
    d. Dynamic
16. User profiles are stored by default in a sub-directory named after the user account in what default directory on a Windows XP Professional system?
    a. \Winnt\Profiles
    b. \Users
    c. \Profiles
    d. \Documents and Settings
17. The user account Properties dialog box from the Local Users and Groups tool can be used to change the password. True or False?
18. The user tools of Windows XP Professional can create and manage both local and global groups. True or False?
19. Local groups can have global groups as members. True or False?

20. Which of the following groups are not configurable?
    a. Administrators
    b. Interactive
    c. Backup Operators
    d. Creator Owner
    e. Authenticated Users
21. What makes a profile mandatory?
    a. Checkbox setting through the user account's Properties dialog box
    b. Storing it locally
    c. Renaming a file with the extension .MAN
    d. By not connecting to a network
22. The effective policy is the result of applying all network- or domain-hosted security policies then finally applying the local security policy. True or False?
23. The local security policy is a collection of what individual policies?
    a. password
    b. account lockout
    c. audit
    d. user rights
    e. computer settings
    f. security options
    g. public key
    h. IP security
24. To prevent malicious users from breaking into your computer system by repeatedly trying to guess a password, what built-in security tool can you use?
    a. Password policy
    b. IP security
    c. Lockout
    d. Encryption
25. What control element in Windows XP is used to assign specific privileged actions to users and groups?
    a. Auditing
    b. User rights
    c. Profiles
    d. Security options

Hands-on Projects

Project 5-1

To import a user account:

This hands-on project requires that a domain be accessible over a network connection.

1. Open the Control Panel (**Start**|**Control Panel**).
2. Double-click **User Accounts**.
3. Click **Add**.
4. In the Add New User Wizard, click **Browse**.
5. Select a user account from the list. Click **OK**.
6. Click **Next**.
7. Select **Standard User** when prompted about the level of access to grant this user, click **Finish**.
8. Notice the imported user appears in the list of users on the User Accounts applet.

Project 5-2

To change group membership of an imported user:

This hands-on project requires that Hands-on Project 5-1 be completed.

1. In the User Accounts applet, select the imported user created in Hands-on Project 5-1.
2. Click **Properties**.
3. On the Group Membership tab, select the **Other** radio button.
4. From the pull-down list, select **Power Users**.
5. Click **OK**.

Project 5-3

To delete a user account:

1. In the User Accounts applet, select the imported user created in Hands-on Project 5-1.
2. Click **Remove**.
3. When asked to confirm, click **Yes**.

Project 5-4

To create a new local user account:

1. Select the **Advanced** tab on the User Accounts applet.
2. Click the **Advanced** button.
3. Select the **Users** node in the console tree of Local Users and Groups.
4. Select **Action|New User**.
5. In the New User dialog box, enter a user name (such as **BobTemp**), full name (such as **Bob Smith**), and description (such as **A temporary account for Bob**).
6. Provide a password and confirm that password.
7. Deselect the **User must change password at next logon** checkbox.
8. Click **Create**.
9. Click **Close**.
10. The BobTemp user account is now listed in the details pane.

Project 5-5

To change group membership for a local user account:

Note: This hands-on project requires that Hands-on Project 5-4 be completed.

1. Select the **BobTemp** user account created in Hands-on Project 5-4.
2. Select **Action|Properties**.
3. Select the **Member Of** tab.
4. Click the **Add** button.
5. Click the **Advanced** button.
6. Click **Find Now**.
7. Select the **Power Users** group.
8. Click **OK**.

9. Click **OK**.
10. Select the **Users** group.
11. Click **Remove**.
12. Click **OK** to close the Properties dialog box.

Project 5-6

To create a local group:

This hands-on project requires that Hands-on Project 5-4 be completed.

1. Select the **Groups** node in the console tree.
2. Select **Action|New Group**.
3. In the New Group dialog box, provide a group name (such as **SalesGrp**) and description (such as **Members of the sales department**).
4. Click **Add**.
5. Click **Advanced**.
6. Click **Find Now**.
7. Select the **BobTemp** user.
8. Click **OK**.
9. Click **OK**.
10. Click **Create**.
11. Click **Close**.

Project 5-7

To delete a group:

This hands-on project requires that Hands-on Project 5-5 be completed.

1. Select the **SalesGrp** created in Hands-on Project 5-5.
2. Select **Action|Delete**.
3. When prompted to confirm, click **Yes**.

4. Close the Local Users and Groups tool, by clicking the **X** button in the upper-right corner of the title bar.
5. Close the User Accounts applet by clicking **OK**.

Project 5-8

To change the Local Security Policy:

1. If not already open, open the Control Panel (**Start|Control Panel**).
2. Double-click the **Administrative Tools** applet icon.
3. Double-click the **Local Security Policy** applet icon.
4. Expand the **Account Policies** node.
5. Select the **Password Policy** node.
6. Select **Enforce password history**.
7. Select **Action|Properties**.
8. In the setting dialog box, set the value to **5**. Click **OK**.
9. Select **Maximum password age**.
10. Select **Action|Properties**.
11. In the setting dialog box, set the value to **60**. Click **OK**.
12. Select **Minimum password age**.
13. Select **Action|Properties**.
14. In the setting dialog box, set the value to **2**. Click **OK**.
15. Select **Minimum password length**.
16. Select **Action|Properties**.
17. In the setting dialog box, set the value to **6**. Click **OK**.
18. Select the **Account Lockout Policy** node.
19. Select **Account lockout counter**.
20. Select **Action|Properties**.
21. In the setting dialog box, set the value to **3**. Click **OK**.
22. Select **Account lockout duration**.
23. Select **Action|Properties**.
24. In the setting dialog box, set the value to **30**. Click **OK**.
25. Select **Reset account lockout counter after**.
26. Select **Action|Properties**.
27. In the setting dialog box, set the value to **15**. Click **OK**.
28. Expand the **Local Policies** node (click the plus sign beside the node).

29. Select the **Audit Policy** node.
30. Select **Audit logon events**.
31. Select **Action|Properties**.
32. In the setting dialog box, select **Failure**. Click **OK**.
33. Select **Audit system events**.
34. Select **Action|Properties**.
35. In the setting dialog box, select **Success and Failure**. Click **OK**.
36. Exit the Local Security Policy by selecting **Console|Exit**.
37. When prompted to save settings, select **Yes**.

Project 5-9

To change user rights:

1. Open the Control Panel (**Start|Control Panel**).
2. Double-click the **Administrative Tools** icon.
3. Double-click the **Local Security Policy** icon.
4. Expand the **Local Policy** node.
5. Select **User Rights Assignment**.
6. Double-click **Add workstations to domain**.
7. Click **Add User or Group**.
8. Click **Advanced**.
9. Click **Find Now**.
10. Locate and select **Power Users**.
11. Click **OK**.
12. Click **OK**.
13. Click **OK**.
14. Close the Local Security Settings dialog box by clicking on the **X** button in the title bar.

Project 5-10

To transfer files and settings using the Files and Settings Transfer Wizard:

This hands-on project requires a blank, preformatted floppy disk, a Windows XP Professional system (this will be labeled as the new system in this project), and another system of Windows 9x, NT, 2000, or XP (this will be labeled as the old system in this project). There must be a network communication link between the two systems; this should be established before starting this project.

1. On the new Windows XP Professional system, open the Files and Settings Transfer Wizard (**Start|All Programs|Accessories|System Tools|Files and Settings Transfer Wizard**). The Welcome screen of the Wizard is displayed.
2. Click **Next**.
3. Select **New computer**. Click **Next**.
4. Select **I want to create a Wizard Disk in the following drive**. Click **Next**.
5. Place a blank formatted floppy into the drive and click **OK**.
6. Once the Wizard Disk creation is complete, you'll see instructions that advise you to take the floppy to the other system, and execute **FASTWiz** before continuing with the Wizard on the new system.
7. Go to the old system, logon with the user account from which you want to transfer files and settings. On the old system, execute FASTWiz.exe from the floppy by selecting **Start|Run**, click **Browse**, use the browse interface to locate the FASTWiz file on the floppy, select it, click **Open**, and click **OK** to execute it. The Files and Settings Transfer Wizard launches.
8. Click **Next**.
9. Select one of the methods to transfer files. This lab assumes you'll be using a network drive, so select the **Other** radio button. Define the path to the folder or drive; use the Browse button if necessary.
10. Click **Next**.
11. On the **What do you want to transfer?** page, select **Settings only**.
12. Click **Next**.
13. You may see a window that indicates that you need to install specific programs on the new system in order for the transfer process to be fully successful. These programs will include applications that are on your old system (such as WinZip, WinAmp, RealAudio, QuickTime Player, Quicken, etc.). Install these programs on the new system before proceeding. Click **Next**.
14. The transfer Wizard begins the collection process and stores the data for transfer in the selected path as defined in step 9. When it is complete, press **Finish**.
15. Go back to the new system.

16. Click **Next**.
17. Select the **Other** radio button, then provide the path to the folder or drive used in step 9; use the Browse button if necessary.
18. Click **Next**.
19. Your files are integrated into the new system. When completed, press **Finish**.
20. You will be prompted to log off for the imported changes to take effect. Click **Yes**.
21. Log back on.
22. You should notice that your desktop and user environment now includes items and configuration settings from your old system.

Case Projects

1. Your notebook computer is attached to a docking station whenever you are in the office. Although your Windows XP Professional notebook does not become a member of the domain when docked, it does have the ability to communicate with the domain. Your docking station hosts a color slide printer. How can you grant access to the printer to domain users when your notebook is docked?
2. You are concerned about file security. Recently a staff member was reprimanded because he restored files to a FAT partition instead of an NTFS partition. The user account is a member of the Backup Administrators group and the Power Users group. Because FAT does not have file-level security, the settings on the files allowed everyone on the network to view the confidential files. How can you change the Local Security Policy to prevent this from occurring in the future?